Практическая работа №1.

Проведение предпроектного обследования информационной системы персональных данных. Определение требуемого уровня защищенности персональных данных

Целью проведения работ по защите персональных данных является разработка и осуществление мероприятий по организации и обеспечению безопасности персональных данных при их обработке, хранении и передаче в информационных системах персональных данных (ИСПДн), в соответствии с требованиями действующего законодательства Российской Федерации.

Безопасность персональных данных при их обработке в ИСПДн может быть обеспечена путем создания системы защиты персональных данных (СЗПДн), включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

Требования к СЗПДн могут быть определены по результатам обследования ИСПДн, моделирования угроз и на основании присвоенного уровня защищенности ИСПДн.

Предпроектное обследование ИСПДн – важнейший этап создания систем информационной безопасности, определяющий как стоимость создаваемой системы защиты, так и ее эффективность. В рамках этого этапа проводится обследование существующих ИСПДн, а также анализ локальных организационно-распорядительных документов оператора, регламентирующих обработку и защиту персональных данных в организации.

Целями проведения обследования являются оценка текущего уровня соответствия ИСПДн требованиям нормативных документов по защите персональных данных, сбор сведений, необходимых для построения СЗПДн, создание замысла и стратегии защиты персональных данных, определение

объема и стоимости работ по внедрению СЗПДн, выработка технических решений по защите персональных данных.

Результатами проведения предпроектного обследования являются:

– отчет об обследовании ИСПДн;

– частная модель угроз безопасности персональных данных (УБПДн);

– техническое задание на создание СЗПДн;

– проекты локальных организационно-распорядительных актов оператора по защите персональных данных;

На этапе предпроектного обследования, как правило, проводятся следующие мероприятия:

– устанавливается необходимость обработки данных в ИСПДн;

– определяется перечень персональных данных, подлежащих защите от несанкционированного доступа;

– определяются условия расположения ИСПДн относительно границ контролируемой зоны (КЗ);

– определяются конфигурация и топология ИСПДн в целом и ее отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

– определяются технические средства и системы, предполагаемые к использованию в разрабатываемой ИСПДн, условия их расположения, общесистемные и прикладные программные средства, имеющиеся и предлагаемые к разработке;

– определяются режимы обработки персональных данных в ИСПДн в целом и в отдельных компонентах;

– определяется требуемый уровень защищенности ИСПДн;

– уточняется степень участия персонала в обработке данных, характер их взаимодействия между собой;

– определяются (уточняются) УБПДн в конкретных условиях функционирования (разработка частной модели угроз).

Важным этапом является определение уровня защищенности ИСПДн. Оно проводится в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными Постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

Постановление Правительства РФ № 1119 устанавливает **4 уровня защищенности персональных данных** в зависимости от:

1) категории обрабатываемых персональных данных;

2) типа актуальных угроз безопасности персональных данных (УБПДн);

3) количества субъектов, чьи персональные данные обрабатываются в ИСПДн;

4) являются ли субъекты персональных данных сотрудниками оператора.

Информационная система является информационной системой, обрабатывающей **специальные категории персональных данных** (ИСПДн-С), если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей **биометрические персональные данные** (ИСПДн-Б), если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей **общедоступные персональные данные** (ИСПДн-О), если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных».

Информационная система является информационной системой, обрабатывающей **иные категории персональных данных** (ИСПДн-И), если в ней не обрабатываются персональные данные, указанные в трех предыдущих случаях.

Определение типа УБПДн, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда.

Под **угрозой безопасности персональных данных** (УБПДн) понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных

(недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Информационная система является информационной системой, обрабатывающей **персональные данные сотрудников оператора**, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, **не являющихся сотрудниками оператора**.

Ниже представлена таблица для определения требуемого уровня защищенности (УЗ) персональных данных.

Таблица 1.1. Определение необходимого уровня защищенности ИСПДн

Тип актуальных угроз	Категория обрабатываемых данных	Персональные данные сотрудников оператора		Персональные данные субъектов, не являющихся сотрудниками оператора	
		< 100 000	≥ 100 000	< 100 000	≥ 100 000
1	ИСПДн-С	УЗ 1	УЗ 1	УЗ 1	УЗ 1
	ИСПДн-Б	УЗ 1	УЗ 1	УЗ 1	УЗ 1
	ИСПДн-И	УЗ 1	УЗ 1	УЗ 1	УЗ 1
	ИСПДн-О	УЗ 2	УЗ 2	УЗ 2	УЗ 2
2	ИСПДн-С	УЗ 2	УЗ 2	УЗ 2	УЗ 1
	ИСПДн-Б	УЗ 2	УЗ 2	УЗ 2	УЗ 2
	ИСПДн-И	УЗ 3	УЗ 3	УЗ 3	УЗ 2
	ИСПДн-О	УЗ 3	УЗ 3	УЗ 3	УЗ 2
3	ИСПДн-С	УЗ 3	УЗ 3	УЗ 3	УЗ 2
	ИСПДн-Б	УЗ 3	УЗ 3	УЗ 3	УЗ 3
	ИСПДн-И	УЗ 4	УЗ 4	УЗ 4	УЗ 3
	ИСПДн-О	УЗ 4	УЗ 4	УЗ 4	УЗ 4

Задание

На основе исходных данных, предоставленных преподавателем, провести анализ ИСПДн и подготовить отчет о практической работе, содержащий:

1. Перечень ИСПДн и их основные характеристики.

Пример оформления:

Название ИСПДн	Категория ИСПДн	Сотрудники/клиенты	Количество обрабатываемых данных
АРМ бухгалтера	ИСПДН-С	Сотрудники	Менее 100000
	ИСПДН-И	Сотрудники	Менее 100000

2. Перечень персональных данных, обрабатываемых в ИСПДн и подлежащих защите (для каждой ИСПДн).

Пример оформления:

АРМ бухгалтера.

ИСПДн - С: меж книжка, лист нетрудоспособности

ИСПДн - И: паспортные данные, трудовая книжка

3. Перечень должностей сотрудников, участвующих в обработке персональных данных.

4. Схему расположения ИСПДн относительно границ контролируемой зоны (КЗ) – на плане этажа (здания) отметить расположение всех технических средств ИСПДн и границы КЗ.

5. Схему локальной вычислительной сети (при наличии), иллюстрирующей связи между конечными сетевыми устройствами, входящими в состав ИСПДн, коммутаторами (концентраторами), маршрутизаторами, межсетевыми экранами и т.п.

6. Схему информационных потоков в ИСПДн.

7. Перечень программных средств, используемых в процессе

обработки персональных данных.

8. Информацию о местах хранения носителей персональных данных, обрабатываемых без использования средств автоматизации.

9. Результат определения уровня защищенности ИСПДн.

Название ИСПДн	Категория ИСПДн	Сотрудники/клиенты	Количество обрабатываемых данных	Тип Угроз	УЗ
АРМ бухгалтера	ИСПДН-С	Сотрудники	Менее 100000		
	ИСПДН-И	Сотрудники	Менее 100000		